AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. – 26. (Cancelled)

27. (New) A method for managing access to a plurality of applications using a central server, comprising:

receiving a user name and a user password of a user from a first application;

generating identity assertion information using the user name and the user password;

generating a first artifact associated with the identity assertion information;

sending the first artifact to the first application;

receiving the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application;

verifying the validity of the first artifact upon receipt from the second application; and

sending the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application.

28. (New) The method of claim 27, further comprising:

receiving a request for a second artifact associated with the identity assertion information from the second application;

generating the second artifact associated with the identity assertion information;

sending the second artifact to the second application;

receiving the second artifact and request for the identity assertion information from a third application, wherein the third application receives the second artifact from the second application;

verifying the validity of the second artifact upon receipt from the third application; and

sending the identity assertion information to the third application, wherein the third application uses the identity assertion information to authorize the user to access the third application.

29. (New) The method of claim 28, wherein the identity assertion information is stored in the central server.

30. (New) The method of claim 27, wherein the first artifact comprises a type code, a source identification, and an assertion identification.

31. (New) The method of claim 30, wherein the first artifact further comprises a server identification.

32. (New) The method of claim 27, wherein the identity assertion information is generated in accordance with a Security Assertions Markup Language (SAML) standard.

33. (New) The method of claim 27, wherein the user name and the user password are obtained by the first application from a web browser.

34. (New) A system for managing access to a plurality of applications comprising:

a processor; and

an identity service provider executing on the processor, configured to:

receive a user name and a user password of a user from a first application;

generate identity assertion information using the user name and the user password;

generate a first artifact associated with the identity assertion information;

send the first artifact to the first application;

receive the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application;

verify the validity of the first artifact upon receipt from the second application; and

send the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application.

35. (New) The system of claim 34, wherein the identity service provided is further configured to:

receive request for a second artifact associated with the identity assertion information from the second application;

generate the second artifact associated with the identity assertion information;

send the second artifact to the second application;

receive the second artifact and request for the identity assertion information from a third application, wherein the third application receives the second artifact from the second application;

verify the validity of the second artifact upon receipt from the third application; and

send the identity assertion information to the third application, wherein the third application uses the identity assertion information to authorize the user to access the third application.

36. (New) The system of claim 34, wherein the identity assertion information is stored in the identity service provider.

37. (New) The system of claim 34, wherein the first artifact comprises a type code, a source identification, and an assertion identification.

38. (New) The system of claim 37, wherein the first artifact further comprises a server identification.

39. (New) The system of claim 34, wherein the identity assertion information is generated in accordance with a Security Assertions Markup Language (SAML) standard.

40. (New) The system of claim 34, wherein the user name and the user password are obtained by the first application from a web browser.

41. (New) A computer readable memory comprising program instructions that, when executed by a processor, implement a method managing access to a plurality of applications using a central server, the method comprising:

receiving a user name and a user password of a user from a first application;

generating identity assertion information using the user name and the user password;

generating a first artifact associated with the identity assertion information;

sending the first artifact to the first application;

receiving the first artifact and a request for the identity assertion information from a second application, wherein the second application receives the first artifact from the first application;

verifying the validity of the first artifact upon receipt from the second application; and

sending the identity assertion information to the second application, wherein the second application uses the identity assertion information to authorize the user to access the second application.

42. (New) The computer readable memory of claim 41, where the method further comprises:

receiving request for a second artifact associated with the identity assertion information from the second application;

generating the second artifact associated with the identity assertion information;

sending the second artifact to the second application;

receiving the second artifact and request for the identity assertion information from a third application, wherein the third application receives the second artifact from the second application;

verifying the validity of the second artifact upon receipt from the third application; and

sending the identity assertion information to the third application, wherein the third application uses the identity assertion information to authorize the user to access the third application.

43. (New) The computer readable memory of claim 41, wherein the identity assertion information is stored in the central server.

44. (New) The computer readable memory of claim 41, wherein the first artifact comprises a type code, a source identification, and an assertion identification.

45. (New) The computer readable memory of claim 44, wherein the first artifact further comprises a server identification.

46. (New) The computer readable memory of claim 41, wherein the identity assertion information is generated in accordance with a Security Assertions Markup Language (SAML) standard.

47. (New) The computer readable memory of claim 41, wherein the user name and the user password are obtained by the first application from a web browser.